WHAT IS CLAIMED IS:

1 Sub Ol 1. A method of facilitating verifiable gaming transactions in a distributed

2 environment, the method comprising:

3   executing nested first- and second-type commit/reveal sequences, wherein the

4   first-type commit/reveal sequence commits an outcome generator to a

5   set of outcomes, and instances of the second-type commit/reveal

6   sequence commit at least each player to a respective index contribution

7   and only thereafter reveal the respective index contributions;

8   selecting from the set of outcomes based on a predefined combination

9   operation on the index contributions; and

10   thereafter revealing the set of outcomes for validation thereof.

1 2. The method of claim 1,

2 wherein the set of outcomes correspond to card values from one or more decks

3   thereof.

1 3. The method of claim 2,

2 wherein the cards values are shuffled.

1 4. The method of claim 2,

2 wherein the card values are unshuffled, but the predefined combination

3   operation further operates on an index contribution of the outcome

4   generator.

1 5. The method of claim 1, wherein the set of outcomes correspond to a set of

2 values at least partially defined by one or more of:

3   a deck of cards;

4   sides of a die;

5   sides of a coin; and

6   slots of a wheel.

1 6. The method of claim 1, wherein the first-type commit/reveal sequence

2 includes:

3 encryption of the set of outcomes;

4 supply of the encrypted set of outcomes to each of the players; and

5 later access to set of outcomes using a key.

1 7. The method of claim 1, wherein the first-type commit/reveal sequence

2 includes:

3 encryption of individual ones of the outcomes;

4 supply of the ordered set of encrypted outcomes to each of the players; and

5 later access to the selected outcomes using respective keys.

1 8. The method of claim 1, wherein the second-type commit/reveal sequence

2 includes:

3 hashing of respective index contribution using a predetermined hash;

4 supply of the hashed index contributions to the outcome generator and to all of

5 the players; and

6 later supply of the index contributions to the outcome generator and to all of

7 the players.

1 9. The method of claim 1,

2 wherein the first- and second-type commit/reveal sequences include respective

3 transformational securings selected from the set of cryptographic

4 encodings, hashes and irreversible transforms.

1 10. The method of claim 1,

2 wherein the first-type commit/reveal sequence is performed substantially by a

3 game processor; and

4 wherein the second-type commit/reveal sequence is performed substantially by

5 respective player processors.

1 11. A verifiable gaming transactions method comprising:

2 transformationally securing an encoding of a predetermined set of outcomes;

3 supplying one or more players with the transformationally secured encoding;

4 receiving a transformationally secured player index from each of the one or

5 more players; and

- 26 -

6   selecting a particular one of the outcomes for revealing to the one or more

7   players based on a combination of the player indices.

1   12. The method of claim 11,

2   wherein the predetermined set of outcomes is transformationally secured using

3   a cryptographic key; and

4   wherein the player indices are transformationally secured using a hash.

1   13. The method of claim 11, further comprising:

2   receiving and verifying the player indices against respective

3   transformationally secured player indices prior to the outcome

4   selecting.

1   14. The method of claim 11, further comprising:

2   randomizing ordering of the predetermined set of outcomes prior to the

3   securing thereof.

1 _Sub 31/7_ 15. The method of claim 11, further comprising:

2   effectively randomizing the set of outcomes by further combining the player

3   indices with the randomized index.

1   16. The method of claim 11,

2   wherein the combination includes a bit-wise exclusive OR of binary encodings

3   of the player indices.

1   17. The method of claim 11,

2   wherein the selecting includes a modulo function.

1 _Sub 32/7_ 18. The method of claim 11,

2   wherein the transformational securing of the randomized set encoding includes

3   cryptographically securing the set of outcomes.

1   19. The method of claim 11,

2   wherein the transformational securing of the randomized set encoding includes

3   cryptographically securing individual outcomes of the set thereof.

1   20. A verifiable gaming transactions method comprising:

2   receiving a transformationally secured encoding of a predetermined set of

3   outcomes for a gaming transaction;

4   supplying a transformationally secured encoding of a player input;

5   after each of zero or more other participants in the gaming transaction has

6   supplied a transformationally secured corresponding input, supplying

7   the player input; and

8   accessing a particular one of the outcomes selected based on a combination of

9   the player input with the corresponding input for each of the zero or

10   more other participants.

1   21. The method of claim 20, further comprising:

2   supplying successive player inputs after prior supply and receipt of

3   corresponding transformationally secured inputs; and

4   accessing successive one of the outcomes selected based on combination of

5   the successively supplied player inputs with the corresponding inputs

6   for each of the zero or more other participants.

1   22. The method of claim 20,

2   wherein the accessing includes receiving an encoding of the particular

3   outcome subject to later verification against the transformationally

4   secured set of outcomes.

1   23. The method of claim 20,

2   wherein outcomes of the transformationally secured set thereof are

3   individually secured; and

4   wherein the accessing includes obtaining a key for a corresponding

5   individually secured outcome.

1   24. The method of claim 20,

Sub 13 3/

- 28 -

2 wherein outcomes of the transformationally secured set thereof are

3 individually secured; and

4 wherein the accessing includes receiving an encoding of the particular

5 outcome for verification against the corresponding individually

6 secured outcome.

1 25. An outcomes generator for verifiable gaming transactions comprising:

2 a commitment sequence executable to supply one or more players with a

3 transformationally secured set of outcomes; and

4 a reveal sequence responsive to receipt of transformationally secured player

5 index contributions from each of the one or more players, the reveal

6 sequence executable to select a particular one of the outcomes based

7 on a combination of the player indices.

1 26. The outcomes generator of claim 25,

2 integrated with, and responsive to, game logic.

1 27. The outcomes generator of claim 25,

2 wherein the commitment and reveal sequences employ cryptographic

3 transformations.

1 28. A player client for verifiable gaming transactions comprising:

2 a commitment sequence executable, after receipt of a transformationally

3 secured encoding of a predetermined set of outcomes, to supplying a

4 transformationally secured encoding of a player input; and

5 a reveal sequence executable, after each of zero or more other participants in a

6 gaming transaction has supplied a transformationally secured

7 corresponding input, to reveal the player input; and

8 a selector for a particular one of the outcomes based on a combination of the

9 player input with the corresponding input for each of the zero or more

10 other participants.

1 29. A computer program product encoded in one or more computer readable

2 media and comprising:

3   first instructions executable by a computing machine as part of a first

4   commit/reveal protocol to supply one or more players with a

5   transformationally secured set of outcomes;

6   second instructions executable by the computing machine to distribute

7   transformationally secured player index contributions from each of the

8   one or more players and only thereafter distribute the index

9   contributions as part of a second commit/reveal protocol nested within

10   the first commit/reveal protocol; and

11   third instructions executable by the computing machine to reveal the set of

12   outcomes.

1   30. The computer program product of claim 29,

2   wherein the one or more computer readable media are selected from the set of

3   a disk, tape or other magnetic, optical, or electronic storage medium

4   and a network, wireline, wireless or other communications medium.

1   31. A method of making a computer-readable encoding of a verifiable gaming

2   outcome, the method comprising:

3   transformationally securing an encoding of a predetermined set of outcomes;

4   supplying one or more players with the transformationally secured encoding;

5   receiving a transformationally secured player index from each of the one or

6   more players;

7   selecting a particular one of the outcomes for revealing to the one or more

8   players based on a combination of the player indices; and

9   encoding as the computer-readable encoding, information usable by the one or

10   more players to reveal the selected outcome.

1   _Sub 847_ 32. The method of claim 1,

2   wherein the information encodes the selected outcome.

1   33. The method of claim 1,

- 30 -

2   wherein the information includes a key to reveal at least the selected one of the

3   outcomes from the supplied transformationally secured encoding

4   thereof.

1   34. The method of claim 1,

2   wherein the computer-readable encoding includes at least one message

3   suitable for communication between a gaming server and a client

4   thereof.

1   35. An apparatus comprising:

2   means for committing to a particular set of outcomes without revealing same;

3   and

4   means for ensuring an irrevocable commitment to respective index

5   contributions by each party to a distributed transaction and only

6   thereafter revealing a particular one of the outcomes based on a

7   combination of the index contributions.

Add Cl